Notice of Allowability	**Application No.** 10/042,019	**Applicant(s)** QI, ZHENG	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *RCE filed on 4/23/2007 and phone interview held on 7/3/2007*.

2. ☒ The allowed claim(s) is/are *1-24*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *7/3/2007* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7, 5, 07

DETAILED ACTION

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Lori A. Gordon and David T. Story on July 3, 2007.

The application has been amended as follows:

Amend the following **claims 1 and 10**.

1. An authentication engine architecture for a SHA-1 multi-round authentication algorithm, comprising:

a hash engine configured to implement hash round logic for a SHA-1 authentication algorithm, the SHA-1 hash round logic ~~implementation~~ including,

a combined adder tree having:

~~with~~ a timing critical path configured to produce a first output, the timing critical path having a single 32-bit carry look-ahead adder (CLA),

a second path, parallel to the timing critical path, configured to produce a second output, the second path having a single CLA, and

a selector configured to select an output [[,]] ~~wherein an output of said combined adder tree is selected~~ from [[an]] the output of the timing critical path and [[an]] the output of [[a]] the second ~~parallel computation~~ path.

10. A method of authenticating data transmitted over a computer network, comprising:

receiving a data packet stream;

splitting the packet data stream into fixed-size data blocks; and

processing the fixed-size data blocks using a SHA-1 multi-round authentication engine architecture, said architecture implementing hash round logic for a SHA-1 authentication algorithm, the SHA-1 hash round logic including :

a combined adder tree having:

~~with~~ a timing critical path configured to produce a first output, the timing critical path having a single 32-bit carry look-ahead adder (CLA),

a second path, parallel to the timing critical path, configured to produce a second output, the second path having a single CLA, and

a selector configured to select an output [[,]] ~~wherein an output of said combined adder tree is selected~~ from [[an]] the output of the timing critical path and [[an]] the output of [[a]] the second ~~parallel computation~~ path.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/23/2007 has been entered.

Response to Arguments

3. In response to communications filed on 4/23/2007, applicant amends claims 1, 2, 10, and 11. The following claims 1-24 are presented for examination.

3.1 Applicant's remarks, filed on 4/23/2007, with respect to the art rejection of claims 1-24 have been fully considered and they are persuasive in light of the Examiner's amendment above.

Allowable Subject Matter

4. The following is an examiner's statement of reasons for allowance: "An Efficient Implementation of Hash Function Processor for IPSEC" to Kang et al, pp. 1-4, the closest of the prior arts of record to the claimed invention teaches implementation of hash functions for IPSEC chip designed to reduce the number of gates. Kang et al discloses a SHA-1 algorithm that takes as input a message with a maximum length of less than 2^{64} bits and produces as output a 160-bit message digest. The input is processed in 512-bit blocks. Kang et al also discloses a SHA-1 architecture structure using a 32-bit data bus and its flow controlled by multiplexers, wherein the right side is the core operation and the left side is the circuit of intermediate value as shown in fig.2. Fig.2 shows four Boolean operators for parallel processing and to minimize the adder delay a high speed adder is implemented using a 8-bit CLA (carry look-ahead adder), CSA (carry select adder, and CSA (carry save adder). Kang et al whether alone or in combination with the other prior arts of record fail to teach

"An authentication engine architecture for a SHA-1 multi-round authentication algorithm, comprising: a hash engine configured to implement hash round logic for a SHA-1 authentication algorithm, the SHA-1 hash round logic including,

a combined adder tree having:

a timing critical path configured to produce a first output, the timing critical path having a single 32-bit carry look-ahead adder (CLA),

a second path, parallel to the timing critical path, configured to produce a second output, the second path having a single CLA, and *a selector configured to select an output from the output of the timing critical path and the output of the second path"* as recited in amended claim 1 and

"A method of authenticating data transmitted over a computer network, comprising:

receiving a data packet stream;

splitting the packet data stream into fixed-size data blocks; and

processing the fixed-size data blocks using a SHA-1 multi-round authentication engine architecture, said architecture implementing hash round logic for a SHA-1 authentication algorithm, the SHA-1 hash round logic including :

a combined adder tree having:

a timing critical path configured to produce a first output, the timing critical path having a single 32-bit carry look-ahead adder (CLA),

a second path, parallel to the timing critical path, configured to produce a second output, the second path having a single CLA, and

a selector configured to select an output from the output of the timing critical path and the output of the second path as recited in amended claim 10.

Consequently claims 2-9 and 11-24 are directly or indirectly dependent upon claims 1 and 10 and therefore, they are also allowable over the prior arts of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C.C./

Carl Colin
Patent Examiner, A.U. 2136
July 3, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

7/5/07